



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/512,403	11/14/2005	Jyrki Maijala	Q84328	4450
23373	7590	05/14/2008	EXAMINER	
SUGHRUE MION, PLLC 2100 PENNSYLVANIA AVENUE, N.W. SUITE 800 WASHINGTON, DC 20037			MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER			
		2131		
MAIL DATE	DELIVERY MODE			
05/14/2008	PAPER			

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/512,403	Applicant(s) MAIJALA ET AL.
	Examiner Aravind K. Moorthy	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 14 November 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-10 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-10 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 25 October 2004 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1668)
 Paper No(s)/Mail Date see attachment.

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application

6) Other: _____

DETAILED ACTION

1. This is in response to the communications filed on 14 November 2005.
2. Claims 1-10 are pending in the application.
3. Claims 1-10 have been rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-4 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claim 1 is directed towards a method of storing sensitive information in a system comprising two databases. The claim recites “receiving a storage request including the information to be stored and first identifier for identifying an individual with whom the information to be stored is associated,” “generating a second identifier in such a manner that its value does not depend on the first identifier,” “storing the first identifier and the second identifier in the first database in such a manner that the first identifier is bound to the second identifier,” and “storing the information to be stored in the second database together with the second identifier. However, it is unclear to the examiner as to which entity is executing the receiving, generating and storing steps. For the sake of examination, the examiner will assume it is a computer (i.e. server or client) that receives the request

Any claims not directly addressed are rejected on the virtue of their dependency.

Claim Objections

5. Claims 5 and 7-10 are objected to because of the following informalities: typographical error. A colon has been omitted after the word “comprising” in the claims. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-10 are rejected under 35 U.S.C. 102(c) as being anticipated by Jeran U.S. Patent No. 6,954,753 B1.

As to claim 1, Jeran discloses a method of storing sensitive information in a system comprising two databases, the method comprising:

receiving a storage request (i.e. Jeran discloses that upon receipt of a user-initiated access request for the logical storage device 34, controller 36 automatically initiates and establishes communications with the remote secure storage facility 14 and transmits the access request to the remote secure storage facility 14) [column 6, lines 21-26] including the information to be stored (i.e. as shown in figure 2 d:\userID\path1\path2\...filename.doc) and a first identifier (i.e. user ID code) [column 6, lines 55-62] for identifying an individual with whom the information to be stored is associated (i.e. Jeran discloses a user is, preferably,

assigned a user identification code (user ID code) which is the identification code for the assigned dedicated data storage unit 20) [column 4, lines 57-59];

generating a second identifier in such a manner that its value does not depend on the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40];

storing the first identifier and the second identifier in the first database (i.e. local storage device 30) in such a manner that the first identifier is bound to the second identifier (i.e. Jeran discloses when submitting an access request, the user would specify only the logical storage device, the "d" drive, for example, and the path elements 44 and 46 without specifying the user ID 42. The logical storage device controller 36 would then attach the appropriate user ID to the access request based on the user submitting the access request prior to transmitting the access request to the remote secure storage facility 14, thus making the user ID also transparent to the user) [column 7, lines 7-14] (i.e. Jeran discloses the filename and reference ID is also transmitted (70) back to the client computer 12 via the communications network 16 and stored (72) in a local data base 74 where the logical storage device controller 36 maintains a directory for each of the user-assigned dedicated data storage units) [column 7, lines 43-48]; and

storing the information to be stored in the second database (i.e. remote storage facility 14) together with the second identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40].

As to claim 2, Jeran discloses a method as claimed in claim 1, further comprising:

checking, before generating the second identifier, in the first database if a second identifier is generated for the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40];

if so, using the second identifier in the first database [column 7, lines 36-40]; and

if not, generating the second identifier [column 7, lines 36-40].

As to claim 3, Jeran discloses a method as claimed in claim 1 further comprising:

receiving a retrieval request (i.e. Jeran discloses in a manner similar to that described with reference to FIG. 3, to submit an access request, the user simply uses the "open file" command conventionally provided by most user applications. When the list of drives is displayed, the user selects the logical storage device, the "d" drive, for example) including the first identifier (i.e. Jeran discloses the user selects (82) the appropriate subdirectory, designated by the user ID code, and the desired data file from the subdirectory) [column 7, lines 63-66];

retrieving the second identifier corresponding to the first identifier from the first database (i.e. Jeran discloses at the remote secure storage facility 14, utilizing the user name, the user ID code and the reference ID, the system processor 22 validates (88) that an authorized user is submitting the access request) [column 8, lines 13-16]; and

retrieving the requested information from the second database using the second identifier (i.e. Jeran discloses at the remote secure storage facility 14, utilizing the user name, the user ID code and the reference ID, the system processor 22 validates (88) that an authorized user is submitting the access request) [column 8, lines 13-16].

As to claim 4, Jeran discloses a step of sending, to the request, a response including the requested information and the first identifier (i.e. Jeran discloses that if the access request is valid (i.e., submitted by an authorized user) the system processor 22 grants access in accordance with the set of instructions associated with the specified user ID code, cross-references the specified reference ID with the filename database 66 and retrieves (92, 68) the desired data file. Using the decryption key 24, the retrieved data file is decrypted removing any encryption provided by the remote secure storage facility at the time the data was stored) [column 8, lines 24-29].

As to claim 5, Jeran discloses a telecommunication server in a data system comprising at least two databases and a system for generating information to be stored, the telecommunication server comprising

reception means for receiving a request (i.e. Jeran discloses that upon receipt of a user-initiated access request for the logical storage device 34, controller 36 automatically initiates and establishes communications with the remote secure storage facility 14 and transmits the access request to the remote secure storage facility 14) [column 6, lines 21-26], the request including the information to be stored and a first identifier for identifying an individual with whom the information to be stored is associated (i.e. as shown in figure 2 d:\userID\path1\path2\...filename.doc);

first processing means for determining a second identifier corresponding to the first identifier in the first database (i.e. local storage device 30) of the data system, the second identifier being generated in such a manner that its value does not depend on the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40]; and

second processing means for storing the information to be stored together with the second identifier in the second database (i.e. remote storage facility 14) of the data system (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data

storage unit 20 identified by the user ID code specified in the access request)
[column 7, lines 36-40].

As to claim 6, Jeran discloses a telecommunication server as claimed in claim 5, wherein
the reception means are also arranged to receive a data retrieval request
and to separate it from the storage request (i.e. Jeran discloses in a manner similar
to that described with reference to FIG. 3, to submit an access request, the user
simply uses the "open file" command conventionally provided by most user
applications. When the list of drives is displayed, the user selects the logical
storage device, the "d" drive, for example) including the first identifier (i.e. Jeran
discloses the user selects (82) the appropriate subdirectory, designated by the user
ID code, and the desired data file from the subdirectory) [column 7, lines 63-66];
and

the second processing means are also arranged to retrieve the data stored
together with the second identifier from the second database of the data system in
response to the data retrieval request and to forward the retrieved data without the
second identifier to the party making the data retrieval request (i.e. Jeran discloses
that if the access request is valid (i.e., submitted by an authorized user) the system
processor 22 grants access in accordance with the set of instructions associated
with the specified user ID code, cross-references the specified reference ID with
the filename database 66 and retrieves (92, 68) the desired data file. Using the
decryption key 24, the retrieved data file is decrypted removing any encryption

provided by the remote secure storage facility at the time the data was stored)
[column 8, lines 24-29].

As to claim 7, Jeran discloses a telecommunication server in a data system comprising at least two databases and a system comprising stored data, the telecommunication server comprising

reception means for receiving a request (i.e. Jeran discloses that upon receipt of a user-initiated access request for the logical storage device 34, controller 36 automatically initiates and establishes communications with the remote secure storage facility 14 and transmits the access request to the remote secure storage facility 14) [column 6, lines 21-26], the request being associated with the stored data and including a first identifier for identifying an individual with whom the stored data is associated (i.e. as shown in figure 2 d:\userID\path1\path2\...filename.doc);

first processing means for determining a second identifier corresponding to the first identifier in the first database (i.e. local storage device 30) of the data system, the second identifier being generated in such a manner that its value does not depend on the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40]; and

second processing means for retrieving the stored data together with the second identifier from the second database (i.e. remote storage facility 14) of the

data system (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40].

As to claim 8, Jeran discloses a network node comprising

a database for storing data (i.e. remote storage facility 14), and reception means for receiving a request (i.e. Jeran discloses that upon receipt of a user-initiated access request for the logical storage device 34, controller 36 automatically initiates and establishes communications with the remote secure storage facility 14 and transmits the access request to the remote secure storage facility 14) [column 6, lines 21-26] directed to the database and for separating a first identifier in the request, the first identifier identifying an individual with whom the data to be stored is associated (i.e. Jeran discloses a user is, preferably, assigned a user identification code (user ID code) which is the identification code for the assigned dedicated data storage unit 20) [column 4, lines 57-59];

generation means for generating a second identifier for the first identifier in such a manner that the value of the second identifier does not depend on the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40];

storage means for storing the first identifier and the second identifier in the database in such a manner that the first identifier is bound to the second identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40]; and

response means for returning the second identifier in response to the request (i.e. Jeran discloses the filename and reference ID is also transmitted (70) back to the client computer 12 via the communications network 16 and stored (72) in a local data base 74 where the logical storage device controller 36 maintains a directory for each of the user-assigned dedicated data storage units) [column 7, lines 43-48].

As to claim 9, A network node as claimed in claim 8, further comprising

processing means for checking if the database comprises a second identifier for the first identifier, and, if not, to trigger the generation means (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40];

wherein the generation means are configured to be responsive to the processing means [column 7, lines 36-40].

As to claim 10, A data system comprising

at least one telecommunication server (i.e. remote storage facility 14, it is well known in the art that a server is a device that performs services for connected clients, in this case the remote storage facility provides the service of a secure electronic storage)

at least a first database (i.e. local storage device 30) comprising records wherein a first identifier identifying an individual is linked to at least one second identifier (i.e. Jeran discloses when submitting an access request, the user would specify only the logical storage device, the "d" drive, for example, and the path elements 44 and 46 without specifying the user ID 42. The logical storage device controller 36 would then attach the appropriate user ID to the access request based on the user submitting the access request prior to transmitting the access request to the remote secure storage facility 14, thus making the user ID also transparent to the user) [column 7, lines 7-14], which alone does not identify the individual and whose value is generated in such a manner that it does not depend on the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40];

at least a second database (i.e. remote storage facility 14) comprising sensitive information stored [column 4, lines 15-25] in such a manner that each piece of personal information is bound to the corresponding second identifier (i.e.

Jeran discloses that the filename includes the reference ID assigned by the system processor 22 when the data file was stored in the dedicated data storage unit 20 identified by the specified user ID code) [column 7 line 66 to column 8 line 2]; wherein

the telecommunication server is arranged to determine a second identifier corresponding to the first identifier in the database in response to a request including the first identifier (i.e. Jeran discloses a filename and reference number (reference ID) is generated and the data file is stored (68) in the assigned dedicated data storage unit 20 identified by the user ID code specified in the access request) [column 7, lines 36-40], to delete the first identifier from the request, to add the second identifier to the request and then to send the request to the second database (i.e. Jeran discloses the filename and reference ID is also transmitted (70) back to the client computer 12 via the communications network 16 and stored (72) in a local data base 74 where the logical storage device controller 36 maintains a directory for each of the user-assigned dedicated data storage units) [column 7, lines 43-48].

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131